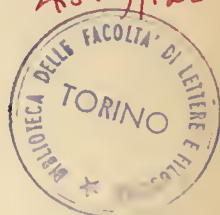


Spacc. PA-I-1284-

THEORIA
DE
CONGRUENTIAS INTRA NUMEROS INTEGRO
PER
MICHAELE CIPOLLA

Congruentias in genere - Theorema de Fermat, de Enlero et
de Wilson - Congruentias de primo gradu - Congruentias
de secundo gradu - Congruentias binomio - Gaussiano,
radices primitivo, indices - Applicationes.



83672

CORILEONE, januario-aprile 1904.

1875-1876

THEORIA

de

CONGRUENTIAS INTRA NUMEROS INTEGRO

per

MICHAELE CIPOLLA

Congruentias in genere - Theorema de Fermat, de Eulero et de Wilson -
Congruentias de primo gradu - Congruentias de secundo gradu -
Congruentias binomio - Gaussiano, radices primitivo, indices - Ap-
plicationes.

In ce scripto me collige, in ordine de tractatione, propo-
sitiones de theoria de congruentias intra numeros integro, que
constitue primo parte de theoria de numeros que me spera
confice postea.

Me adde et aliquo notitia historico et bibliographico, ut
que lege pote cognosce origine et progressu de theoria et adhibe
operas que contine suo explicatione.

Me non arroga ad me ut assequer propositio omnino in per-
fecto modo, sed me spera revertit ad incepto ut commuta et
corrige, et adpone additamento sive in propositiones sive in
notitia historico et bibliographico. Ideo me pete benevolentia et
favore de omni que excole et dilige tali parte de Analysisi,
que cum optimo iure Gauss appella regina de Mathematica
et me es laeto recipere consilio de omni genere.

Operas

que tracta de theoria de congruentias

A. M. LEGENDRE, *Essai sur la théorie des nombres*. Paris
1^{re} éd. an VI (1798); 2^e éd. 1808; 3^e éd. 1830; réimpression fac-
simile de la troisième éd, Paris: Hermann, 1899 — Translatio
in lingua germanico per H. MASER ex 3 ed., Leipzig 1886; ex
2 ed. Leipzig 1893.

C. F. GAUSS, *Disquisitiones arithmeticae*, Lipsiae, 1801 (=
= Werke t. I) — Translatio in franco de POULLET-DELISLE

(*Recherches arithmétiques*, Paris, 1807) — Traduzione in lingua germanico de H. MASER (*Untersuchungen über höhere Arithmetik*, Berlin, 1889).

L. POINSOT, *Réflexions sur les principes fondamentaux de la théorie des nombres*, Journal de Liouville, t. X, 1845.

P. L. TCHEBYCHEF, *Theoria de congruentias* (in russo), S. Petroburgo, 1847. — Traduzione in lingua germanico per H. SCHAPIRA, Berlin 1889. — Traduzione in italico per I. MASSARINI, Roma 1895.

V. A. LEBESGUE, *Exercices d'Analyse numérique*, Paris 1859; *Introduction à la Théorie des nombres*, Paris 1868.

H. I. ST. SMITH, *Report on the Theory of Numbers*, British Assoc. for the advancement of Sc., 1859, p. 228; 1860, p. 120; 1861, p. 292; 1863, p. 168; 1865, p. 322 = Coll. Math. Papers t. I., p. 38, 93, 163, 229, 263, 289.

P. LEJEUNE-DIRICHLET, *Vorlesungen über Zahlentheorie*, herausgegeben von R. DEDEKIND, Braunschweig, 1. Auf. 1863, 2. Auf. 1871, 3. Auf. 1879, 4. Auf. 1894. — Traduzione in italico ex 3 ed. per A. FAIFOFER, Venezia, 1881. — Traduzione in russo, parte 1, per J. M. NASARJEWY, S. Petroburgo, 1899.

J. A. SERRET, *Cours d'Algèbre Supérieure*, 4^e éd., 2 v., Paris 1877, 5^e éd., 1885.

— Traduzione in lingua germanico per G. WERTHEIM, Leipzig 1878.

G. WERTHEIM, *Elemente der Zahlentheorie*, Leipzig, 1887.

J. SOCHOTZKY, *Algebra Supérieure*, v. 2, *Fundamenta de theoria de numeros* (in russo), S. Petroburgo, 1888.

T. J. STIELTJES, *Sur la theorie des nombres. Etude bibliographique*. Ann. de Toulouse, IV, 1890, pp. 1-103; Paris, Gauthier-Villars, 1895.

E. LUCAS, *Théorie des Nombres*, t. I. Paris 1891. (Alto tomo non es publicato pro morte de auctore).

P. BACHMANN, *Die Elemente der Zahlentheorie*, Leipzig, 1892.

G. B. MATHEWS, *Theory of Numbers*, Part. I, Cambridge 1892.

U. SCARPIS, *Primi elementi della Teoria dei numeri*, Milano, Hoepli, 1897.

E. CAHEN, *Elements de la Théorie des nombres*, Paris. 1900.

P. BACHMANN, *Niedere Zahlentheorie*, Enzykl. d. math. wiss. t. I, pp. 551-581. — I Teil, Leipzig, pp. X + 402, 1902.

L. KRONECKER, *Vorlesungen über Mathematik*; 2 Teil, *Vorlesungen über allgemeine Arithmetik*; hrsg. von K. HENSEL, 1 Absch., *Vorlesungen über Zahlentheorie*, 1 Band, Leipzig, 1901.

G. WERTHEIM, *Anfangsgründe der Zahlenlehre*, Braunschweig, 1902.

P. GAZZANIGA, *Gli elementi della teoria dei numeri*, Padova, Frat. Drucker, 1903.

§ 1 Congruentias in genere

* 1. $m, n \in \mathbb{N}_1, a, b, c, d \in \mathbb{N} \supset$:

$$a \equiv b + mn \equiv c \pmod{m} \implies a - b \equiv mn \pmod{m}$$

GAUSS scribe relatione $a \equiv b + mn$ ita

$$a \equiv b \pmod{m}$$

et voca illo « congruentia »: « Si numerus a numerorum b, c differentiam metitur, b et c secundum a congrui dicuntur, sin minus, incongrui: ipsum a modulum appellamus. Uterque numerorum b, c , priori in casu alterius residuum, in posteriori vero non residuum vocatur » (D. A., art. 1.).

LEGENDRE scribe $a \equiv b + M(m)$ et es contrario ad symbolo et denominatione de GAUSS: « Ces équations entre des restes... se traitent comme les équations ordinaires, sans qu'il soit besoin des signes nouveaux d'égalité ni des dénominations nouvelles assez incongrues, dont quelques géomètres font usage ». (*Essai*, etc., 2^e éd., 2^e suppl., p. 12, note).

CATALAN seque notatione de LEGENDRE: « Admirables (les Recherches Arithmétiques de Gauss) sauf les dénominations et la notation. POULLET-DELISLE, traducteur de Gauss, dit qu'elles peuvent étonner. De son côté, LEGENDRE s'est raillé des expressions incongrues, adoptées par le Géomètre de Brunswick. Mais LEGENDRE et DELISLE avaient des oreilles françaises » (v. *Mélanges mathématiques* par E. C. CATALAN, in Mémoires de la Société Royale des Sciences de Liège, t. XIII, s. 2, 1886, p. 334).

Hodie denominatione et symbolo de GAUSS es communi ad maximo parte de auctore, sed non es necessario introduc novo

symbolo in ce scripto, quod notatione $a \varepsilon b+mn$ es satis simplice.

- 2 $a \varepsilon b+mn . b \varepsilon c+mn \supset . a \varepsilon c+mn$
- 3 ————— $\supset . a+c \varepsilon b+c+mn$
- 31 ————— $\supset . a-c \varepsilon b-c+mn$
- 4 ————— $. c \varepsilon d+mn \supset . a+c \varepsilon b+d+mn$
- 41 ————— $\supset . a-c \varepsilon b-d+mn$
- 5 ————— $\supset . ac \varepsilon bc+mn$
- 51 ————— $. c \varepsilon d+mn \supset . ac \varepsilon bd+mn$
- 52 ————— $. r \varepsilon N_0 \supset . a^r \varepsilon b^r+mn$
- 6 $ac \varepsilon bc+mn \supset . a \varepsilon b+[m/D(c,m)]n$
- 7 $(b+mn) \wedge (b+nn) = b+mlt(m,n) \times n$
- 8 $a \varepsilon b+nD(m,n) \supset . \neg (a+nm) \wedge (b+nn)$
- 9 $a \varepsilon b+nD(m,n) \supset . (a+nm) \wedge (b+nn) =$
 $a+m\{n \wedge \exists [mx/D(m,n) \varepsilon (b-a)/D(m,n)+nn/D(m,n)]\}$
- 91 $D(m,n)=1 \supset . (a+nm) \wedge (b+nn) = a+nm \wedge (b-a+nn)$

§ 2 Residuo de funciones particulares

* 2. $p \varepsilon N_p . m, n \varepsilon N_1 \supset$:

- 1 $C(m,n) \varepsilon C[\text{quot}(m,p), \text{quot}(n,p)] \times$
 $\times C[\text{rest}(m,p), \text{rest}(n,p)] + pn$
- 2 $C(m,n) \varepsilon \Pi[C\{\text{rest}[\text{quot}(m,p^r)], \text{rest}[\text{quot}(n,p^r), p]\} | r, N_0] + np$
- 21 $m, n \varepsilon np \supset . C(m,n) \varepsilon C[\text{quot}(m,p), \text{quot}(n,p)] + np$
- 22 $n \varepsilon 1 \cdots (p-1) \supset . C(p,n) \varepsilon N_1 \times p$

{LEIBNIZ, Math. Schr., t.7, p.102}

- 23 $n \varepsilon 0 \cdots (p-1) \supset . C(p-1,n) \varepsilon (-1)^n + N_0 \times p$
- 24 $n \varepsilon 0 \cdots (p-2) \supset . C(p-2,n) \varepsilon (-1)^n (n+1) + N_0 \times p$

$$\cdot 25 \quad n \in 0 \dots (p-3) \quad \supset \quad C(p-3, n) \in (-1)^n (n+1)(n+2)/2 + N_0 \times p$$

$$\cdot 26 \quad p \in N_{p-12} \quad n \in 2 \dots (p-1) \quad \supset \quad C(p+1, n) \in N_1 \times p$$

{2·1·2...26, LUCAS, *American J. a.* 1878, t. I. p. 229, et *Théorie des nombres*, 1891, pp. 417-420}

P2·22 = Form. 1902, p. 72, 12·7 . ·23 = F, p. 72, 12·71 . ·24 = F, p. 72, 12·73 . ·26 = F, p. 72, 12·72.

$$\ast \quad 3. \quad p \in N_p \quad m \in N_1 \quad \supset:$$

$$\cdot 1 \quad m \in (p-1) \times N_0 \quad \supset \quad \Sigma [1 \dots (p-1)]^m \in N_1 \times p$$

{LIONNET, v. CATALAN, *Mém. de l'Ac. de Belgique*, t. 46, 1886, p. 14}

$$\cdot 2 \quad m \in (p-1) \times N_0 \quad \supset \quad \Sigma [1 \dots (p-1)]^m \in -1 + N_1 \times p$$

$$\cdot 3 \quad p \in N_p \quad p > 3 \quad \supset \quad nt \Sigma [1 \dots (p-1)] \in p^2 \times N_1$$

{OSBORN, 1892, *The Messenger of Math.*, t. 22, p. 51}

$$\cdot 4 \quad p \in N_p \quad p > 3 \quad \supset \quad nt \Sigma [1 \dots (p-1)]^2 \in p \times N_1$$

{GLAISHER, 1900, *Quarterly Journ. of Math.* t. 31, p. 337}

P3·1 = F, p. 138, 20·1 . ·3 = F, p. 138, 20·1 . ·4 = F, p. 138, 20·2.

§ 3 Theorema de Fermat, de Eulero et de Wilson

$$\ast \quad 4. \quad m \in N_1 \quad p \in N_p \quad a \in n \quad \supset:$$

$$\cdot 1 \quad D(a, m) = 1 \quad \supset \quad a \nmid \Phi m \in 1 + mn$$

Ce propositionne es dicto « theorema de EULERO », nam illo pertine ad EULERO, que primo stude functione Φ (EULER, *Novi Comm. Acad. Sc. Petrop.* a. 1760-61, t. 8, pp. 85-103, *Act. Ac. Sc. Petrop.* a. 1780, t. 4, p. 18; Φm = numero de numeros que non supera m et es primo cum m). Symbolo Φ es introducto a GAUSS (1801, *Werke* t. 1 p. 30); EULERO ute simbolo H (*Acta Ac. Sc. Petrop.*, 1780, p. 18). LUCAS (*T. de Nombres*, 1891) voca illo *indicatore*, vocabulo introducto a CAUCHY (*Oeuvres*, s. 1, t. 6, p. 124) in sensu paueo differente).

$$\cdot 11 \quad a \in np \quad \supset \quad a^{p-1} \in 1 + np$$

Ce theorema maxime elegante et fundamentali in theoria de congruentias es appellato *theorema de Fermat*, quod FERMAT

primo (a. 1640) enuntia illo (v. Oeuvres, Paris 1891, t.2 p. 209). LEIBNIZ primo demonstra illo (Math. Schr. t. 7, p. 154), sed suo demonstratione non es noto in tempore de GAUSS (v. D. A., p. 54 nota).

EULERO publica primo demonstratione in Comm. Ac. Sc. Petrop., t. 8, p. 143 (a. 1736), et altero in Novi Comm. Ac. Sc. Petrop., t. 8, p. 70. Vide et LAMBERT, Acta Eruditorum, a. 1769, p. 109; Gauss, D. A. art. 49-51; LEGENDRE, Essai etc, 2^e éd., n. 129.

Secundum HEANS (Messenger of Math., a. 1898, t. 27, p. 174), Mathematicos sinense novi ce theorema, per $a=2$, e tempore de CONFUCIO (CON-FU-TSE) a. —550 — —447; sed illos puta es vero propositione inverso:

$$p \in N_1 \cdot 2^p - 2 \in N_1 \times p \supset p \in N_p,$$

quod es falso (v. meo scripto: Sui numeri composti che verificano la congruenza di Fermat $a^{p-1} \equiv 1 \pmod{p}$, Ann. di Mat., a. 1903, t. 9, s. 3, pp. 139-160; v. et P 49, 50 de ce scripto).

$$^2 \quad m \in (N_1 + 4) - N_p \supset (m-2)! \in N_1 m$$

$$^3 \quad (p-2)! \in 1 + N_0 \times p$$

$$\{2^3 \text{ LEIBNIZ, Mss. Mat. t.3 B11 fol. 10}$$

$$^4 \quad (p-1)! \in -1 + N_1 \times p$$

Ce propositione es dicto « theorema de WILSON », quod WARING, (*Meditationes Algebrae* ed. I., a. 1770, p. 218; ed. III, a. 1782, p. 382), attribue illo ad WILSON, suo discipulo. Primo demonstratione de ce P. pertine ad LAGRANGE (Nouv. Mém de l'Ac. de Berlin, a. 1771, t. 2, p. 125 = Oeuvres, t. 3, p. 425). EULERO trade novo demonstratione in *Opuscula analytica*, S. Petr. a. 1783, t. 1., p. 329), GAUSS alio in Disquis. arith., art. 77 et alio LEGENDRE in Essai, 2^e ed. n. 130.

Theorema de WILSON es casu particulari de propositione circa numeros primo que pertine ad J. STEINER (J. f. Math. t. 13, a. 1835, p. 356 = Werke t. 2, p. 7: vide et JACOBI, ibidem t. 14, a. 1835, p. 64 = Werke t. 6, p. 262).

$$^5 \quad p \in N_p \Rightarrow p \in N_1 + 1 \cdot (p-1)! + 1 \in N_1 \times p$$

$$^6 \quad p \in 4N_1 + 1 \supset \{[(p-1)/2]!\}^2 \in -1 + N_1 \times p$$

$$\cdot 7 \quad p \in 4N_1 - 1 \quad \supset \quad \{[(p+1)/2]!\}^2 \in 1 + N_1 \times p$$

(P · 6 · 7 es enuntiatio in *Meditationes algebrae de* WARING (a. 1770) sed demonstratione pertine ad LAGRANGE (a. 1771, Oeuvres, t. 3, p. 431) Vide et LEGENDRE, Essai, 2^e éd, n. 131.:

P · 7 pote es enuntiatio

$$p \in 4N_1 - 1 \quad \supset \quad [(p+1)/2]! \in (1 + N_1 \times p) \setminus (-1 + N_1 \times p)$$

Quaestione de investiga in quali casu residuo de $[(p+1)/2]!$, sequente modulo p , es congruo 1 aut -1 , posito a LEJEUNE-DIRICHLET (J. f. Math., t. 3, a. 1828, p. 401 = Werke t. 1, p. 105) es resolutio a JACOBI (ibidem, t. 9, 1832, p. 189 = Werke t. 6, p. 240), que trade ce propositione

$$p \in 4N_1 - 1 \quad \supset \quad [(p+1)/2]! \in (-1)^{\text{Num}[(p+1)/2 \cdots p \wedge n^2 + np]} \\ \text{KRONECKER et LIOUVILLE da alio regulas minus simplice [J. de Math (2), t. 5, 1860, p. 127, 267]}$$

$$\cdot 8 \quad m \in (Np - t2) \text{N}_1 \vee 2[(Np - t2) \text{N}_1] \vee t4 \quad \supset \quad$$

$$H\{1 \cdots m \wedge x3[D(x, m) = 1]\} \in -1 + N_1 m$$

$$\cdot 9 \quad m \in N_1 - t4 - (Np - t2) \text{N}_1 - 2[(Np - t2) \text{N}_1] \quad \supset \quad$$

$$H\{1 \cdots m \wedge x \in [D(x, m) = 1]\} \in 1 + N_1 m$$

P · 8 · 9 constitue « theorema de WILSON amplificato ». GAUSS (D. A. art. 70) enuntia illo et da aliquo notione circa demonstratione, pro que vide BRENNECKE, CRELLE et ARNDT, J. f. Math., t. 19, a. 1839, p. 319; t. 20, a. 1840, p. 29, et t. 31, a. 1846, p. 329.

P4·1 F. 1902, p. 143, P·2 · 11 F. p. 71, P·2 · P4·2 F. p. 72, 12·1 · 3 F. p. 72, 12·2 · 4 F. 12·3 · 5 F. 12·4 · 6 F. 12·5 · 7 F. 12·6.

* 5.

$$\cdot 0 \quad m \in N_1 + 1 - 8N_1 \quad \supset \quad \Psi_m = \text{mlt}[\Phi x | x, (Np \text{N}_1) \wedge m/N_1] \quad \text{Df}$$

$$\cdot 01 \quad m \in 8N_1 \cdot n \in \text{mp}(2, m) \quad \supset \quad$$

$$\Psi_m = \text{mlt}\{2^{n-2}, \Phi x | x, [(Np - t2) \text{N}_1] \wedge m/N_1\} \quad \text{Df}$$

$$\cdot 02 \quad \Psi 1 = 1 \quad \text{Df}$$

$$\cdot 1 \quad m \in N_1 \quad \supset \quad \Psi_m \in N_1 \wedge m/N_1$$

$$\cdot 2 \quad m \in N_1 - t4 - (Np - t2) - 2[(Np - t2) \text{N}_1] \quad \supset \quad \Psi_m < \Phi m$$

Ψ_m = indicatore reducto de m , v. LUCAS, Théorie des Nombres, 1891, p. 428

$$\cdot 3 \quad p \in Np - t2 \cdot a, b \in n - np \cdot r, s \in N_1 \cdot a \in b + p_r(n - np) \quad \supset \quad$$

$$a \nmid p^s \in b \nmid p^s + p^{r+s}(n - np)$$

$$\cdot 31 \quad a, b \in 2n+1 \cdot r, s \in N_1+1 \cdot a \in b+2^r(2n+1) \cdot \supset \cdot \\ a^s \in b^s+2^{4+s}(2n+1)$$

$$\cdot 32 \quad a \in 2n+1 \cdot s \in N_1+2 \cdot \supset \cdot a \nmid 2^{s-2} \in 1+2^s n \\ (V. \text{ GAUSS, Disq. Arith. art. 90.})$$

$$\cdot 4 \quad a \in n \cdot m \in N_1 \cdot D(a, m) = 1 \cdot \supset \cdot a \nmid \Psi_m \in 1 + mn$$

$$\cdot 5 \quad a \in n \cdot m \in N_1 \cdot n = \max[\text{mp}(x, a) | x, Np] \cdot \supset \cdot \\ a \nmid (n + \Psi_m) \in a \nmid n + mn \\ (\text{LUCAS, Th. d. N., p. 430})$$

§ 4 Congruentias de primo gradu

* 6. $a, b \in n \cdot m \in N_1 \cdot \supset :$

$$\cdot 1 \quad b \in n = nD(a, m) \cdot \supset \cdot \neg \exists n \wedge x \exists (ax + b \in mn)$$

$$\cdot 2 \quad b \in nD(a, m) \cdot \supset \cdot n \wedge x \exists (ax + b \in mn) = \\ n \wedge x \exists [(ax + b)/D(a, m) \in mn/D(a, m)]$$

$$\cdot 3 \quad b \in nD(a, m) \cdot \supset \cdot \text{Num}[0 \cdots (m-1) \wedge x \exists (ax + b \in mn)] = D(a, m)$$

$$\cdot 4 \quad D(a, m) = 1 \cdot \supset \cdot n \wedge x \exists (ax + b \in mn) = -ba \nmid (\Psi_m - 1) + mn$$

$$\cdot 41 \quad p \in Np \cdot D(a, p) = 1 \cdot \supset \cdot n \wedge x \exists (ax + b \in np) = -ba^{p-2} + mn$$

In ce propositiones es methodo ut investiga solutione de congruentia de primo gradu. Secundum P 441 metodo trahe origine ex theorema de Fermat (411) et de Eulero (41) aut ex propositione 54. Congruentia de primo gradu pote es resolutio cum methodo ut resolve aequatione indeterminato de primo grado, p. ex. cum auxilio de fractione continuo, ut fac LAGRANGE (Histoire de l'Ac. de Berlin, a. 1767, p. 175). Vide et GAUSS, Disq. Arith., art. 26-31, LEGENDRE, Essai, 2^e éd., § 11.

GAUSS (Disq. Arith., art. 31) scribe numeros que satisfac ad relatione $ax \in b + mn$ sub forma $\frac{b}{a} \pmod{m}$. Ce expressione habe aut nullo aut uno aut plure valore incongruo \pmod{p} . Hodie maximo parte de auctore non ute ce notatione de GAUSS.

* 7. $n \in N_1 . m \in N, F1 \dots n . a \in (n-1)F1 \dots n . \supset$:

$$\cdot 1 \quad r, s \in 1 \dots n . r < s . \supset_{r,s} D(m_r, m_s) = 1 : u = \Pi(m_s | 1 \dots n) . \\ k \in nF1 \dots n : r \in 1 \dots n . \supset_{r,k} k \in n \wedge x \in (xu/a_r \in 1 + m_r n) : \supset : \\ n \wedge x \exists (r \in 1 \dots n . \supset_{r,x} x \in a_r + nm_r) = \Sigma (a_r k_r u / m_r | r, 1 \dots n) + nu$$

$$\cdot 2 \quad \exists n \wedge x \exists (r \in 1 \dots n . \supset_{r,x} x \in a_r + m_r n) . = : r, s \in 1 \dots n . \supset_{r,s} . \\ a_r - a_s \in nD(m_r, m_s)$$

$$\cdot 3 \quad n_1 = \Pi [x \nmid \text{mp}(x, m_1) | x, \text{Np} \wedge x \exists (r \in 2 \dots n . \supset_{r,x} \text{mp}(x, m_1) \nmid \text{mp}(x, a_r)) . r \in 2 \dots n . n_r = \Pi [x \nmid \text{mp}(x, m_r) | x, \text{Np} \wedge x \exists (s \in 1 \dots n - 1 . \supset_s . \\ \text{mp}(x, m_r) > \text{mp}(x, a_s)) . \supset : r, s \in 1 \dots n . r < s . \supset . D(n_r, n_s) = 1 . \\ \Pi(n_r | r, 1 \dots n) = \text{mlt}(a_r | r, 1 \dots n)$$

$$\cdot 4 \quad \text{Hp} \cdot 2 \cdot 3 . \supset . n \wedge x \exists (r \in 1 \dots n . \supset_{r,x} x \in a_r + nm_r) = \\ = n \wedge x \exists (r \in 1 \dots n . \supset_{r,x} x \in a_r + nm_r)$$

Ce propositiones, que constitue règles de GAUSS (*Disq. Arith.* art. 32-36), es in antiquo libro de arithmetica de sinense Sum Tszc; v. K. D. BIERNATZKI, *J. f. Math.*, t. 52, a. 1856, p. 59; MATTHIESSEN, ibidem, t. 91, 1881, p. 254. STIELTJES (*Ann. de Toulouse*, t. 4, 1890) tracta ce quaestione cum maximo claritate.

§ 5 Congruentias de secundo gradu

* 8. $a, b, c \in n . p \in \text{Np} - 2 . D(a, p) = 1 . \supset$:

$$\cdot 1 \quad n \wedge x \exists (ax^2 + bx + c \in np) = n \wedge x \exists [\exists n \wedge x \exists (x^2 \in b^2 - 4ac + np) . \\ 2ax + b \in x + np]$$

{GAUSS, *Disqu. Arith.* art. 152}

$$\cdot 2 \quad a \nmid [(p-1)/2] \in -1 + np . \supset . \neg \exists n \wedge x \exists (x^2 \in a + np)$$

$$\cdot 3 \quad a \nmid [(p-1)/2] \in 1 + np . \supset . \exists n \wedge x \exists (x^2 \in a + np) \\ \{2 \cdot 3 \text{ EULERO, } \textit{Opus. anal.} \text{ t. 1, a. 1773, p. 242. 268} = \textit{Comm. Arith. coll.} \text{ t. 2, p. 1, 13; GAUSS, } \textit{Disqu. Arith.} \text{ art. 106; LEGENDRE, } \textit{Essai, 2^e \text{éd.} n. 134}\}$$

$$\cdot 32 \quad a \nmid [(p-1)/2] \in 1 + np . \supset . \text{Num}[1 \dots (p-1) \wedge x \exists (x^2 \in a + np)] = 2$$

$$\cdot 32 \quad \text{—————} . k \in 1 \dots (p-1) \wedge x \exists (x^2 \in a + np) . \supset . \\ ik \cup i(p-k) = 1 \dots (p-1) \wedge x \exists (x^2 \in a + np)$$

* 9. $p, q \in \mathbb{N}_p - 2$. $a, b \in \mathbb{N}$. \supset :

$$\cdot 0 \quad J(a, p) = 1 \quad . = . \quad a \in (\mathbb{N}^2 + \mathbb{N}p) - \mathbb{N}p \quad \text{Df}$$

$$\cdot 01 \quad J(a, p) = -1 \quad . = . \quad a \in \mathbb{N}^2 + \mathbb{N}p \quad \text{Df}$$

$$\cdot 02 \quad J(a, p) = 0 \quad . = . \quad a \in \mathbb{N}p \quad \text{Df}$$

$\cdot 03 \quad J(a, p) \in \{1, -1, 0\} \wedge \exists x \{a \mid [(p-1)/2] \in x + \mathbb{N}p\} \quad \text{Dfp}$
 {LEGENDRE (*Essai*, éd 2^e, n. 155) indica residuo de $a \mid [(p-1)/2]$

(mod p) cum symbolo $\left(\frac{a}{p}\right)$, que hodie es communi ad omni auctore, sed apud LEGENDRE tali symbolo habe aut valore 1 aut valore -1 , nam definitione $\cdot 03$ es posteriore. Nos ute simbolo $J(a, p)$, que es magis consentaneo ad notatione de Form.}

$$\cdot 1 \quad J(1, p) = 1$$

$$\cdot 2 \quad J(-1, p) = (-1)^{\lfloor (p-1)/2 \rfloor}$$

$\cdot 21 \quad J(-1, p) = 1 \quad . = . \quad p \in 4\mathbb{N}_0 + 1 : J(-1, p) = -1 \quad . = . \quad p \in 4\mathbb{N}_0 + 3$
 {Ce theorema es noto ad FERMAT, sed primo demonstratione pertine ad EULERO (*Opusc. Anal.* t. 1. p. 64, *Comm. Petrop.* n. 5, a. 1759, p. 5, et n. 18, a. 1774, p. 112 = *Comm. Ar.* coll. 1, p. 210, 477) Vide et GAUSS, *Disq. Arith.*, art. 108-111,}

$$\cdot 3 \quad J(ab, p) = J(a, p) \times J(b, p)$$

$$\cdot 4 \quad a \in b + \mathbb{N}p \quad \supset . \quad J(a, p) = J(b, p)$$

$$\cdot 5 \quad J(2, p) = (-1)^{\lfloor (p^2-1)/8 \rfloor}$$

$$\cdot 51 \quad J(2, p) = 1 \quad . = . \quad p \in (8\mathbb{N}_0 + 1) \cup (8\mathbb{N}_0 + 7):$$

$$J(2, p) = -1 \quad . = . \quad p \in (8\mathbb{N}_0 + 3) \cup (8\mathbb{N}_0 + 5)$$

{ $\cdot 5 \cdot 51$ FERMAT novi ce theorema sed non trade demonstratione. (*Op. math.*, p. 168). EULERO fac conatu ut demonstra illo sed frustra. Primo demonstratione rigoroso pertine ad LAGRANGE (*Nouv. Mém. de l'Ac. de Berlin*, a. 1775. pag. 349, 351 = *Oeuvres* t. 3, p. 771. Vide et GAUSS, *Disq. Arith.* art. 112, 116, LEGENDRE, *Essai*, 2^e éd. n. 148, 386; STIELTJES, *Neuw Arch.* t. 9, a. 1882, p. 193, *Ann. d. Toulouse*, t. 11 A, a. 1887, p. 5.

$$\cdot 6 \quad J(3, p) = 1 \quad . = . \quad p \in (12\mathbb{N}_0 + 1 \cup 12\mathbb{N}_0 + 11):$$

$$J(3, p) = -1 \quad . = . \quad p \in (12\mathbb{N}_0 + 5 \cup 12\mathbb{N}_0 + 7)$$

$$\cdot 7 \quad J(5, p) = 1 \quad . = . \quad p \in (20\mathbb{N}_0 + 1 \cup 20\mathbb{N}_0 + 9 \cup 20\mathbb{N}_0 + 11 \cup 20\mathbb{N}_0 + 19):$$

$$J(5, p) = -1 \quad . = . \quad p \in (20\mathbb{N}_0 + 3 \cup 20\mathbb{N}_0 + 7 \cup 20\mathbb{N}_0 + 13 \cup 20\mathbb{N}_0 + 17)$$

$$\begin{aligned} \cdot 8 \quad J(7, p) &= 1. =. p \varepsilon (28N_0 + 1 \cup 28N_0 + 3 \cup 28N_0 + 9 \cup 28N_0 + 19 \cup \\ &28N_0 + 25 \cup 28N_0 + 27): \\ J(7, p) &= -1. =. (28N_0 + 5 \cup 28N_0 + 11 \cup 28N_0 + 13 \cup 28N_0 + 15 \\ &\cup 28N_0 + 17 \cup 38N_0 + 23) \end{aligned}$$

†6·7·8 Ce propositiones que es casu particiari de « lege de reciprocitate de residuos quadratico » (10·4) es noto multo ante que demonstratione de ce theorema. P·6 circa residuo 3 es noto ad FERMAT (*Opera math.* t. 2, p. 857) sed EULERO primo demonstra illo et « eo magis es mirandum demonstrationem propositionum ad residua +2 et -2 pertinentium, prorsus similibus artificiis innexas, semper ipsius sagacitatem fugisse » (GAUSS, *Disqu. Arith.* art. 120). LAGRANGE postea demonstra ee P et P·7·8 circa residuo 5 et 7, sed illo non investiga ultra (*Mémoires de l'Ac. de Berlin* 1775, p. 352);. Vide et BRICARD, *Sur le caractère quadratique du nombre 3* etc., *Nouv. Ann. s. 3^e, t. 16*, a. 1887, p. 546{.

✱ 10. $p, q \varepsilon Np-2 . a, b \varepsilon n . \supset$:

$$\cdot 1 \quad a \varepsilon b + np . \supset . J(a, p) = (-1)^{\sum [E(2ra/p)]r, 1 \cdots (p-1)/2}$$

{LEGENDRE, *Essai*, 2^e éd. nn. 381, 382{

$$\cdot 2 \quad a \varepsilon 2N_0 + 1 - N_1 \times p . \supset . J(a, p) = (-1)^{\sum [E(ra/p)]r, 1 \cdots (p-1)/2}$$

{LEGENDRE, *Essai*, 2^e éd. nn. 383, 384{

$$\cdot 3 \quad J(q, p) = (-1)^{\text{Num}\{1 \cdots (p-1)/2 \wedge x3[\text{rest}(xq, p) > p/2]\}}$$

« Lemma de Gauss » (*Werke* t. 2, p. 3) - Ce P es extenso a P. GAZZANIGA in R. Istituto Veneto s. 6, 4², 1886, p. 1271.

$$\cdot 31 \quad J(q, p) = \text{sgn} \Pi \{ [xq/p - E(xq/p + 1/2)] | x, 1 \cdots (p-1)/2 \}$$

$$\cdot 32 \quad J(q, p) = \text{sgn} \Pi \{ [\sin(2xq\pi/p)] / \sin(2x\pi/p) | x, 1 \cdots (p-1)/2 \}$$

{EISENSTEIN, *J. f. Math.* t. 29, a. 1845, p. 177.}

$$\cdot 33 \quad J(q, p) = \Pi \{ \Pi [(h/p - k/q)(h/p + k/q - 1/2) | h, 1 \cdots (p-1)/2] | k, 1 \cdots (q-1)/2 \}$$

$$\cdot 34 \quad J(q, p) = \Pi \{ \Pi [(h/p - k/q) | h, 1 \cdots (p-1)/2] | k, 1 \cdots (q-1)/2 \}$$

{KRONECHER, *Berlin. Ber.* t. 7, a. 1884, p. 519{

$$\cdot 4 \quad J(p, q) = (-1)^{\sum [(p-1)(q-1)/4]} \times J(q, p)$$

{Ce propositione es « lege de reeiprocitate de residuos quadratico » EULERO inveni illo sed non demonstra :

« Existente s numero quocumque primo, dividantur tantum quadrata imparia

1, 9, 25, 49,...

per divisorem $4s$, notenturque residua, quae omnia erunt formae $4q+1$, quorum quodvis littera a indicetur, reliquorum autem numerorum, formae $4q+1$, qui inter residua non occurrunt, quilibet littera A indicetur, quo facto si fuerit divisor numerus primus

| formae | tum est |
|---------|--|
| $4ns+a$ | $+s$ residuum et $-s$ residuum |
| $4ns-a$ | $+s$ residuum et $-s$ non-residuum |
| $4ns+A$ | $+s$ non-residuum et $-s$ non-residuum |
| $4ns-A$ | $+s$ non-residuum et $-s$ residuum ». |

(Opusc. Anal., t. 1, a. 1772).

Primo demonstratione pertine ad LEGENDRE, sed non est rigoroso. GAUSS trade septem demonstratione de ce « theorema fundamentali » :

1°. demonstratione (Disqu. Arith. art. 131-151) es ducto cum methodo de inductione ex theorema

$$p \in 8N_3+1 \quad \supset \quad \exists Np \wedge 1 \cdots (p-1) \wedge x3[J(p,x) = -1].$$

2°. demonstratione (Disqu. Arith. art. 262) es deducto ex theoria de formas quadratico ;

4°. et 6°. (Werke, t. 2, p. 9 et 55) ex teoría de divisione de circulo ;

7°. (Werke, t. 2, p. 234) ex theoria de congruentias de gradu superiore ;

3°. et 5°. ex P 10·3 (lemma de GAUSS).

EISENSTEIN (J. f. Math, t. 28, a. 1844, p. 246) da demonstratione geometrico.

GENOCCHI (Mém. de l'Ac. de Belgique, t. 25, a. 1853 (1852), cap. 13; vide et Comptes Rendus de l'Ac. de Paris t. 90, a. 1880, p. 350; et J. f. Math, 1892) funda simplice demonstratione de lege de reciprocitate supra relatione

$$2E(hq/p) = \sum \{ [1 + \text{sgn}(h/p - k/q)] | k, 1 \cdots (q-1)/2 \},$$

$$2E(hq/p+2) = \sum \{ [1 + \text{sgn}(h/p + k/q - 2)] | k, 1 \cdots (q-1)/2 \}$$

(Circa relationes analogo v. HACKS, Acta Math, t. 12, 1888, p. 109; BUSCHE, Ueber eine Beveismethode in der Zahlentheorie, Göttingen, 1883; STEIN, J. f. Math, t. 106, a. 1890, p. 337).

Circa alio simplice demonstratione v. BUNIAKOWSKY, Bull. St-Pét., t. 14, a. 1869, p. 432; — ZELLER, Monatsberichte der Ber. Ak., a. 1872; — ZOLOTAREFF, Nouvelles Annales, s. 2, t. 11, a. 1872, p. 354; — SCHERING, Gött. Nachr. a. 1879, p. 217.

KRONECKER publica vario articulo circa lege de reprocitate (V. Kronecker's Werke). Simplicissimo es demonstratione de ce auctore, posito supra P. 10:33:34 (Berl. Berichte, t. 7, a. 1884, p. 519).

Ad publicationes citato nos adde

KRONECKER, Berl. Monatsber, a. 1880, p. 686, p. 854; — SYLVESTER, Comptes Rendus de l'Ac. de Paris, t. 90, a. 1880, p. 1053, 1104; t. 91, p. 154; — THOMAE, Zeitsch. f. Math. v. Ph, t. 26, a. 1881, p. 134; — STELTJES, Nieuw Arch. t. 9, a. 1882, p. 193; — SCHERING, Acta Math, t. 1, a. 1883, p. 153; — KRONECKER, Berl. Ber., a. 1884, p. 519; J. f. Math., t. 96, a. 1884, p. 348; Berl. Ber., a. 1884, p. 645; J. f. Math., t. 97, a. 1884, p. 93; Berl. Ber. a. 1885, p. 383; — GEGENBAUER, Wien Ber. t. 91, a. 1885, p. 11; t. 92, a. 1885, p. 876; — SCHERING, Berl. Ber., a. 1885, p. 113; — KRONECKER, Berl. Ber., a. 1885, p. 117; — KUMMER, J. f. Math., t. 100, a. 1886, p. 10; — HERMES, Hoppe Arch., t. 5, a. 1887, p. 190; — LERCH, Teixeira J., t. 8, a. 1887, p. 137; — GEGENBAUER, Wien Ber. t. 97, a. 1888, p. 427; — BUSCHE, J. f. Math., t. 103, a. 1888, p. 118; — KRONECKER, J. f. Math., t. 104, a. 1889, p. 348; — TAFELMACHER, Diss. Göttingen, a. 1889; — LIPSCHITZ, C. R. de l'Ac. de Paris, t. 108, a. 1889, p. 489; — MANDL, Monatsber. f. Math., t. 1, a. 1890, p. 465; — PÉPIN, Acc. Pont. dei N. Lincei, t. 43, a. 1890, p. 192; — FRANKLIN, Messenger of Math., t. 19, a. 1890, p. 176; — FIELDS, American J. t. 13, a. 1890, p. 189; — BUSCHE J. f. Math., t. 106, a. 1890, p. 65; — KRONECKER, J. f. Math., t. 106, a. 1890, p. 346; — MATROT, Assoc. Franç., Limoges XIX, a. 1890, p. 79; — LUCAS, Assoc. Franç., Limoges XIX, a. 1890, p. 147; Mélanges math. et astr., S. Pétersb. t. 7, 1891, p. 65; — GEGENBAUER, Wien Ber, t. 100, a. 1891, p. 855; p. 1072; — SCHMIDT, J. f. Math., t. 111, a. 1893, p. 107; GEGENBAUER, Wien Ber., t. 103, a. 1894, p. 285; — BANG, Nyt Tidss. for Math., t. 5 B., a. 1894, p. 92; — BUSCHE,

Hamb. Mitt. t. 3, a. 1896, p. 233; — LANGE, Leipz. Ber., t. 48, a. 1896, p. 629; — LERCH, Bull. Int. Prague, 1896; — LANGE, Leipz. Ber., t. 49, a. 1897, p. 607; — STERNEK, Recueil math. de Moscou. (in russo), t. 20, a. 1898, p. 267; — PÉPIN, Acc. P. d. N. Lincei, t. 51, a. 1898, p. 123; — ALEXEJEVSKY, Charkow Ges. t. 6, 1898, p. 200 (in russo); PÉPIN, Mem. Acc. d. N. Lincei, t. 16, a. 1900, p. 229; — FISCHER, Monatsb., f. Math. t. 11, a. 1900, p. 176; — GAUSS, *Sechs Beweise des Fundamentaltheorems über quadratische reste*, hrsg. von NETTO, (Ostwalds kl. N^o 122), Leipzig: W. Engelmann, a. 1901.

* 11. $a, b \in n. m, n \in 2N_0 + 1 \rightarrow$

·0 $J(a, m) = II[J(a, p) | p, Np \wedge m/N_1]$ Df
 $J(a, m)$ es appellato symbolo de Jacobi.

·01 $J(a, -m) = J(a, m)$ Df

·1 $J(a \times b, m) = J(a, m) \times J(b, m)$

·2 $a \in b + np \rightarrow J(a, m) = J(b, m)$

·3 $J(1, m) = 1$

·4 $J(-1, m) = (-1)^{[(m-1)/2]}$

·5 $J(2, m) = (-1)^{[(m^2-1)/8]}$

·6 $a \in N_1 \rightarrow J(a, m) = \text{sgn} II\{\text{rest}(a, m) - m\} | r, 1 \dots (m-1)/2 \wedge$
 $ax \{\text{rest}(xa, m) > m/2\}$ Dfp

{Ita SCHERING et KRONECKER defini symbolo de JACOBI (Berl. Ber. a. 1876, p. 330)

·7 $m \in n. J(a, m) =$
 $II\{[\sin(2ax\pi/m)/\sin(2x\pi/m)] | x, 1 \dots (\text{mod } m-1)/2\}$ Dfp

·8 $m, n \in 2N_0 + 1 \rightarrow J(m, n) =$
 $II\{II[4\sin(h\pi/m + k\pi/n) \times$
 $\sin(h\pi/m - k\pi/2)] | h, 1 \dots (m-1)/2\} | k, 1 \dots (n-1)/2\}$

·9 $m, n \in 2N_0 + 1 \rightarrow J(m, n) = (-1)^{[(m-1)(n-1)/4]} \times J(n, m).$

{9. Extensione de (P10·4) lege de reciprocitate. Ut pote determina valore de $J(m, n)$ es regulas posito aut supra algorithmo de Euclide aut supra algorithmo de fractione continuo, v. GAUSS, Werke, t. 2, p. 61 et sequ.; EISENSTEIN, J. f. Math.,

t. 27, a. 1844, p. 317; LEBESGUE, J. de Math., t. 12, a. 1847, p. 497; ZELLER, Gött. Nach., a. 1879, p. 197; SCHERING, Gött. Nach., a. 1879, p. 217; GEGENBAUER, Wien Berich., a. 1880, p. 931, et a. 1881, p. 1089., KRONECKER, Berl. Ber., a. 1884, p. 530; HEINITZ, Diss. Gött., a. 1893{.

* 12. $p \in N_{p-2} \cdot r, n \in n \cdot J(r, p) = 1 \cdot J(n, p) = -1 \cdot \supset$:

Num{1... $(p-1) \wedge x3[J(x, p) = 1 \cdot J(r+x, p) = 1]$ } = $E[(p-2)/4]$
 Num{1... $(p-1) \wedge x3[J(x, p) = 1 \cdot J(r+x, p) = -1]$ } = $E[(p+2)/4]$
 Num{1... $(p-1) \wedge x3[J(x, p) = -1 \cdot J(r+x, p) = 1]$ } = $E[(p-1)/4]$
 Num{1... $(p-1) \wedge x3[J(x, p) = -1 \cdot J(r+x, p) = -1]$ } = $E[(p-1)/4]$
 Num{1... $(p-1) \wedge x3[J(x, p) = 1 \cdot J(n+x, p) = 1]$ } = $E[(p-1)/4]$
 Num{1... $(p-1) \wedge x3[J(x, p) = 1 \cdot J(n+x, p) = -1]$ } = $E[(p-1)/4]$
 Num{1... $(p-1) \wedge x3[J(x, p) = -1 \cdot J(n+x, p) = 1]$ } = $E[(p+2)/4]$
 Num{1... $(p-1) \wedge x3[J(x, p) = -1 \cdot J(n+x, p) = -1]$ } = $E[(p-2)/4]$
 v. meo scripto *Un metodo per la risoluzione*, etc. Napoli R. 1903,

p. 154.

$p \in N_{p-2} \cdot \supset \cdot \mathfrak{A} 1... (p-1) \wedge x3[J(x, p) = 1 \cdot J(x+1, p) = -1]$
 $p \in N_p \wedge N_1+3 \cdot \supset \cdot \mathfrak{A} 1... (p-1) \wedge x3[J(x, p) = -1 \cdot J(x+1, p) = 1]$
 $\frac{\quad}{\quad} \cdot \supset \cdot \mathfrak{A} 1... (p-1) \wedge x3[J(x, p) = J(x+1, p) = -1]$
 $p \in N_p \wedge N_1+5 \cdot \supset \cdot \mathfrak{A} 1... (p-1) \wedge x3[J(x, p) = J(x+1, p) = 1]$

* 13.1 $p \in N_p \wedge 8N_0+3 \cdot \supset$.

Num{1... $(p-3)/4 \wedge x3[J(x, p) = 1]$ } = $(p-3)/8$

2. $p \in N_p \wedge 8N_0+7 \cdot \supset$.

Num{ $(p-3)/4... (p-3)/2 \wedge x3[J(x, p) = 1]$ } = $(p+1)/8$

1.2 BRICARD, Intermédiaire des M., t. 3, a. 1896, p. 62; t. 6, a. 1902, p. 417{

* 14.1 $m \in 2N_1+1 - N_1 \times N_1^2 \cdot a \in n^2+nm - nm \cdot$

$u \in 1 \wedge (-1)FN_p \cdot \supset$.

Num{1... $(m-1) \wedge n^2-a+nm \wedge x3[p \in N_p \wedge m/N_1 \cdot \supset_p \cdot$

$J(x, p) = u_p \}$ = $\Pi\{E[(p-u_p)/4] \mid p, N_p \wedge m/N_1\}$

{v. meo scripto *Applicazione della teoria* etc., Napoli R., a. 1904, p. 135{

.11

* 15. $p \in N_{p-2} : a \in n \cdot J(a, p) = 1 \cdot \supset$:

1. $p \in 4N_0+3 \cdot \supset \cdot \mathfrak{A} \uparrow[(p+1)/4] \varepsilon n \wedge x3(x^2 \varepsilon a+np)$

- 2 $p \in 8N_0 + 5$. $a \nmid [(p-1)/4] \varepsilon 1 + np$. \supset .
 $a \nmid [(p+3)/8] \varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- 3 ——— . $a \nmid [(p-1)/4] \varepsilon -1 + np$. \supset .
 $2 \nmid [(p-1)/4] \ a \nmid [(p+3)/8] \varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- {·1·2·3 LEGENDRE, *Essai*, 2^e éd., n. 185{
- 4 $p \in 8N_0 + 5$. \supset . $a \nmid [(p+3)/8] \times \{ a \nmid [(p-1)/4] + 3 \nmid [(p-1)/4] \varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- {TONELLI, Lincei R., a. 1892, 1^o sem., p. 116{
- * 16. $p \in N_{p-1/2}$. $a, b \in n$. $J(a, p) = 1$. $J(b, p) = -1$.
 $m \in 2N_0 + 1$. $r, s \in N_1$. $p = 2^s m + 1$. \supset :
- 1 $u \in N_1 \wedge xz(a^m b^{2^s m} \varepsilon 1 + np)$. \supset .
 $b^m \ a \nmid [(m+1)/2] \varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- 2 $k \varepsilon n \wedge xz[J(x+1, p) = 1 \cdot J(x-1, p) = -1] \cdot v \in FN_0$.
 $v_0 \varepsilon k + a \nmid (2^{s-2} m) + np$. $r, \varepsilon k + a \nmid (2^{s-r-2} m) \times$
 $II[r_k \nmid (2^{s-r-h-1} m) | h, 1 \dots (r-1)] + np$
 \supset . $a \nmid [(m+1)/2] \ II[v \nmid (2^r m) | r, 0 \dots (s-1)] \varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- {·1·2 TONELLI, Lincei R., a. 1892, 1^o sem., p. 116{
- 3 $p \in 4N_0 + 1$. $k \varepsilon n \wedge xz(x^2 \varepsilon a + np)$. \supset .
 $kl \nmid (2^{s-2} m) \varepsilon n \wedge xz(x^2 \varepsilon -a + np)$
- {TONELLI, Lincei R., a. 1892, 1^o sem., p. 116{
- * 17. $p \in N_{p-1/2}$. $k, a \in n$. $J(a, p) = 1$. $J(k^2 - a, p) = -1$. \supset :
- 1 $\{ [k + \sqrt{k^2 - a}] \nmid [(p+1)/2] + [k - \sqrt{k^2 - a}] \nmid [(p+1)/2] II \}$
 $\varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- 2 $\sqrt{a} (k + \sqrt{a}) \nmid [(p-1)/2] - (k - \sqrt{a}) \nmid [(p-1)/2] \{ / 2$
 $\varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- {·1·2 v. meo scripto *Un metodo*, etc., Napoli R., a. 1903, p. 154{
- 3 $2 \Sigma \{ a^r \Sigma [1 \dots (p-1) 2]^{2r-1} | r, 1 \dots (p-1)/2 \} \varepsilon n \wedge xz(x^2 \varepsilon a + np)$
- {v. meo scripto *Formole*, etc., Napoli R. a. 1905, p. 13{

Propositiones de nn. 15, 16, 17 enuntia vario methodo ut resolve congruentia de secundo gradu cum modulo primo. GAUSS trade duo methodo ut inveni solutiones, altero (Disqu. Arith., art. 319-322), dicto methodo de *excludente*, exige cognitione de non residuo de plure numero, altero (Disqu. Arith. art. 327) nite in theoria de formas quadratico. Methodos ut

inveni numeros positivo, que non supera modulo et satisfac ad congruentia (*radices*), exige plure conatu et methodo de excludente es in tali casu magis idoneo que omni alio. Ut inveni uno quolibet solutione suffice ute formulas de TONELLI (16·2), aut meo (17·1 vel 17·2), pro que conatus es pauco. Meo formula 17·3 monstra postea solutione de congruentia sine ullo conatu, sed illo es pauco utili in practica.

* 18. $n \in N_1$. $p \in N_{p-2}$. $a \in n$. $J(a, p) = 1$. $\varepsilon \nmid n \wedge x_3(x^2 \varepsilon a + np)$. \supset :

1. $r \varepsilon [(l + \sqrt{a})^n - (l - \sqrt{a})^n] / (2\sqrt{a}) + np$.

$s \varepsilon [(l + \sqrt{a})^n + (l - \sqrt{a})^n] / 2 + np$. \supset .

$n \wedge x_3(x^2 \varepsilon a + np^n) = n \wedge \{x_3(rx \varepsilon s + np^n) \vee x_3(rx \varepsilon -s + np^n)\}$

{LEGENDRE, *Essai*, 2^e éd. n. 187}

2. $(\sqrt[n]{p^{n-1}})a \nmid [(p^n - 2p^{n-1} + 1)/2] \varepsilon n \wedge x_3(x^2 \varepsilon a + np^n)$

{TONELLI, *Lincei R.*, a. 1893, 1^o sem., p. 259}

* 19. $n \in N_1$. $p \in N_{p-2}$. $a \in n$. $J(a, p) = 1$. \supset :

1. $p \varepsilon 4N_0 + 3$. \supset . $a \nmid [(p^n - p^{n-1} + 2)/4] \varepsilon n \wedge x_3(x^2 \varepsilon a + np^n)$

2. $p \varepsilon 8N_0 + 5$. \supset .

$\{a \nmid [(p^n - p^{n-1} + 4)/8]\} \{a \nmid [(p-1)/4] + 3\} \{[(p^n - p^{n-1})/4] \varepsilon$

$n \wedge x_3(x^2 \varepsilon a + np^n)\}$

{1·2 TONELLI, *Lincei R.*, a. 1893, 1^o sem., p. 259}

* 20. $Hp19$. $m \varepsilon 2N_0 + 1$. $r, s \in N_1$. $p = 2^r m + 1$. \supset :

1. $b \varepsilon n$. $J(b, p) = -1$. $u \varepsilon N_1 \wedge x_3\{[a \nmid (p^{n-1}m)]b \nmid (2p^{n-1}mx) \varepsilon$
 $1 + np^n\}$. \supset . $[b \nmid (p^{n-1}mu)]a \nmid [(p^{n-1}m + 1)/2] \varepsilon n \wedge x_3(x^2 \varepsilon a +$
 $np^n)$

{TONELLI, *Lincei R.*, a. 1892, 1^o sem. p. 116}

2. $k \varepsilon n \wedge x_3[J(x+1, p) = 1 \wedge J(x-1, p) = -1] \wedge v \varepsilon nFN_0$.

$v_0 \varepsilon k + a \nmid (2^{s-2}m) + np$. $v_r \varepsilon k + np + [a \nmid (2^{s-r-2}m)] \times$

$II[v_h \nmid (2^{s-r-h-1}m) | h, 1 \dots (r-1)]$. \supset . $\{a \nmid [(p^{n-1}m + 1)/2]\} \times$

$II[v_r \nmid (2^r p^{n-1}m) | r, 0 \dots (s-1)] \varepsilon n \wedge x_3(x^2 \varepsilon a + np^n)$

{TONELLI, *Lincei R.*, a. 1893, 1^o sem. p. 259}

3. $k \varepsilon n$. $J(k^2 - a, p) = -1$. \supset .

$\{a \nmid [(p^n - 2p^{n-1} + 1)/2]\} \{[k + \sqrt{k^2 - a}] \nmid [p^{n-1}(p+1)/2] +$

$[k - \sqrt{k^2 - a}] \nmid [p^{n-1}(p+1)/2]\} \varepsilon n \wedge x_3(x^2 \varepsilon a + np^n)$

- 4 Hp'3. $\bigcup. \sqrt{a} \{ (k + \sqrt{a}) [p^{n-1}(p-1)/2] - (k - \sqrt{a}) [p^{n-1}(p-1)/2] \} / 2$
 $\varepsilon n \wedge x_3(x^2 \varepsilon a + n p^n)$
- {3·4 v. meo scripto *Applicazione*, etc., Napoli R., a. 1904, p. 135}
- * 21. $n \varepsilon N_1 + 1 . p \varepsilon N_{p-2} . k \varepsilon n \wedge x_3(x^2 \varepsilon a + n p^{n-1}) . \bigcup :$
- 1 $b \varepsilon n \wedge x_3[(k^2 - a)/p^{n-1} + 2kx \varepsilon n p] . \bigcup .$
 $a + b p^{n-1} \varepsilon n \wedge x_3(x^2 \varepsilon a + n p^n)$
- * 22·1 $a \varepsilon 2n + 1 . \bigcup : n \wedge x_3(x^2 \varepsilon a + 2n) = 2n + 1$
- 2 $a \varepsilon 4n + 1 \vee 4n - 1 . \bigcup . n \wedge x_3(x^2 \varepsilon a + 4n) = 4n + 1 \vee 4n + 3$
- 3 $a \varepsilon 8n + 1 . \bigcup . n \wedge x_3(x^2 \varepsilon a + 8n) = 8n + 1 \vee 8n + 3 \vee 8n + 5 \vee 8n + 7$
- 4 $r \varepsilon N_0 . \bigcup : \exists n \wedge x_3(x^2 \varepsilon a + 2^{r+3}n) . = . a \varepsilon 8n + 1$
- 5 $r \varepsilon N_0 . a \varepsilon 8n + 1 . \bigcup . \text{Num}[1 \cdots (2^{r+3} - 1) \wedge x_3(x^2 \varepsilon a + 2^{r+3}n)] = 4$
- 6 Hp'5 . $u \varepsilon n \wedge x_3(x^2 \varepsilon a + 2^{r+3}n) . \bigcup . n \wedge x_3(x^2 \varepsilon a + 2^{r+3}n) =$
 $(u + 2^{r+2}n) \wedge (-u + 2^{r+2}n)$
- {6 v. GAUSS *Disqu. Arith.* art. 103; LEGENDRE, *Essai*, 2^e éd. n. 189}
- 7 $a \varepsilon 8n + 1 . m \varepsilon N_1 . s = \text{mp}(2, a - 1) . \bigcup .$
 $1 + (a - 1)/2 \sum \{ C(2r, r) [(1 - a)/4]^r / (r + 1) | r, 0 \cdots E[(m - 2)/(s - 2) - 1] \}$
 $\varepsilon n \wedge x_3(x^2 \varepsilon a + 2^m n)$
- {7 Ce formula pertine ad LEGENDRE (*Essai*, 2^e éd. nn. 350-2); circa
demonstratione rigoroso de illo v. meo scripto: *Estensione
di un metodo di Legendre*, etc., Napoli R., 1905.}
- * 23 $m \varepsilon N_1 . a \varepsilon n . D(a, m) = 1 . \bigcup :$
- 1 $m \varepsilon 2N_0 + 1 \vee 2(2N_0 + 1) . \bigcup : \exists n \wedge x_3(x^2 \varepsilon a + nm) . = .$
 $p \varepsilon N_{p-2} \wedge m/N_1 . \bigcup_p . J(a, p) = 1$
- 11 Hp'1 . $\bigcup . \text{Num}[1 \cdots (m - 1) \wedge x_3(x^2 \varepsilon a + nm)] =$
 $2^p \text{Num}(N_{p-2} \wedge m/N_1)$
- 2 $m \varepsilon 4(2N_0 + 1) . \bigcup : \exists n \wedge x_3(x^2 \varepsilon a + nm) . = : a \varepsilon 2n + 1 :$
 $p \varepsilon N_{p-2} \wedge m/N_1 . \bigcup_p . J(a, p) = 1$
- 21 Hp'2 . $\bigcup . \text{Num}[1 \cdots (m - 1) \wedge x_3(x^2 \varepsilon a + nm)] =$
 $2^p [1 + \text{Num}(N_{p-2} \wedge m/N_1)]$
- 3 $m \varepsilon 8N_1 . \bigcup : \exists n \wedge x_3(x^2 \varepsilon a + nm) . = . a \varepsilon 8n + 1 :$
 $p \varepsilon N_{p-2} \wedge m/N_1 . \bigcup_p . J(a, p) = 1$

$$\cdot 34 \quad \text{Hp} \cdot 3 \quad \supset. \text{Num}[1 \cdots (m-1) \wedge xz(x^2 \varepsilon a + nm)] = \\ 2 \uparrow [2 + \text{Num}(\text{Np} \wedge 2 \wedge m / N_1)]$$

$$\ast \quad 24. \quad m \varepsilon 2N_1 + 1 \quad a \varepsilon n^2 + nm - nm \quad k \varepsilon n \quad n \varepsilon N_0 \quad u, v \varepsilon nFN_0 \\ u_n = [k + \sqrt{(k^2 - a)}]^n - [k - \sqrt{(k^2 - a)}]^n / [2\sqrt{(k^2 - a)}] \\ v_n = [k + \sqrt{(k^2 - a)}]^n + [k - \sqrt{(k^2 - a)}]^n$$

$$\cdot 1 \quad m \varepsilon 3N_1 \quad k \varepsilon n \wedge xz \{ p \varepsilon \text{Np} \wedge m / N_1 \} \supset_p. J(x^2 - a, p) = \\ (-1)^{\uparrow[(p+1)/2]} \\ r = \text{mlt}\{p \uparrow [\max(p, a) - 1] \mid p, \text{Np} \wedge a / N_1 \} \\ \supset. a \uparrow [(\Phi m - r + 1)/2] v_r / 2 \varepsilon n \wedge xz(x^2 \varepsilon a + nm)$$

$$\cdot 2 \quad k \varepsilon n \wedge xz \{ p \varepsilon \text{Np} \wedge a / N_1 \wedge 4N_0 + 3 \} \supset_p. x^2 - a \varepsilon np \wedge \\ xz(p \varepsilon \text{Np} \wedge a / N_1 \wedge 4N_0 + 1) \supset_p. J(x^2 - a, p) = -1 \} \\ m_1 = \text{mlt}\{p \uparrow [\max(p, a) - 1] \mid p, \text{Np} \wedge a / N_1 \wedge 4N_0 + 3 \} \\ m_2 = \text{mlt}\{(p+1)/2 \mid p \uparrow [\max(p, a) - 1] \mid p, \text{Np} \wedge a / N_1 \wedge 4N_0 + 1 \} \\ r = \text{mlt}(m_1, m_2) \supset. a \uparrow [(\Phi m - r + 1)/2] v_r / 2 \varepsilon n \wedge xz(x^2 \varepsilon a + nm)$$

\cdot 1 \cdot 2 \quad v. \text{ meo scripto } *Applicazione*, etc, Napoli R., a. 1904, p. 135\}

§ 6 Congruentias binomio

$$\ast \quad 25. \quad a, m, n \varepsilon N_1 \quad \supset.$$

$$\cdot 1 \quad n \wedge xz(x^m \varepsilon 1 + na \quad x^n \varepsilon 1 + na) = n \wedge xz[x \uparrow D(m, n) \varepsilon 1 + na]$$

$$\cdot 2 \quad n \wedge xz(x^n \varepsilon 1 + na) = n \wedge xz[x \uparrow D(n, \Psi a) \varepsilon 1 + na]$$

$$\ast \quad 26. \quad n \varepsilon N_1 \quad p \varepsilon \text{Np} \wedge 2 \quad \supset:$$

$$\cdot 1 \quad n \wedge xz(x^n \varepsilon 1 + np) = n \wedge xz[x \uparrow D(n, p-1) \varepsilon 1 + np]$$

$$\cdot 2 \quad \text{Num}[(1 \cdots (p-1) \wedge xz(x^n \varepsilon 1 + np))] = D(n, p-1)$$

\{ GAUSS, *Disqu. Arith.* art. 60 et sequentes; LEGENDRE, *Essai* etc., 2^e éd., n. 334\}

$$\cdot 3 \quad k \varepsilon n \wedge np \quad \supset. k \uparrow [(p-1)/D(n, p-1)] \varepsilon n \wedge xz(x^n \varepsilon 1 + np)$$

\{ LEGENDRE, *Essai* etc., 2^e éd. n. 336\}

$$\cdot 4 \quad n \varepsilon N_1 \wedge (p-1) / N_1 \quad u \varepsilon n \quad n = \min[N_1 \wedge xz(u^w \varepsilon 1 + np)] \quad \supset. \\ n \wedge xz(x^n \varepsilon 1 + np) = (u^r + np) \mid r, 1 \cdots n$$

\{ GAUSS, *Disqu. Arith.*, art. 65, 1^o; LEGENDRE, *Essai* etc., 2^e éd., n. 336, 3^o. \}

* 27. $m, n \in \mathbb{N}_1 . p \in \mathbb{N}_{p-1} . \supset$:

- 1 $n \wedge x_3(x^n \varepsilon 1 + np^m) = n \wedge x_3(x \uparrow D[n, p^{m-1}(p-1)] \varepsilon 1 + np^m)$
 - 2 $n \in \mathbb{N}_1 \wedge p^{m-1}(p-1) / \mathbb{N}_1 . \supset . n \wedge x_3(x^n \varepsilon 1 + np^m) =$
 $\{x + yp \uparrow [m - mp(p, n)] + np^m \{x, 1 \cdots (p^m - 1) \wedge x_3[x^n \varepsilon 1 + np^m .$
 $\mathbb{Q} x_3(z^n \varepsilon 1 + np . x \varepsilon z + np)\}, y, 0 \cdots [p \uparrow mp(p, n) - 1]$
 - 3 $\text{Num}[1 \cdots (p^m - 1) \wedge x_3(x^n \varepsilon 1 + np^m)] = D[n, p^{m-1}(p-1)]$
 - 4 $a \in n \wedge x_3(x^n \varepsilon 1 + np^{m-1}) . r = mp(p, n) . \supset$
 $r < n - 1 . h \in n \wedge x_3[(a^n - 1) / p^{m-1} + x a^{n-1} n / p^r \varepsilon np] . \supset .$
 $a + h p^{n-r-1} \varepsilon n \wedge x_3(x^n \varepsilon 1 + np^m)$
 - 5 $a \in n \wedge x_3(x^n \varepsilon 1 + np^{m-1}) . mp(p, n) = n - 1 . \supset .$
 $n \wedge x_3(x^n \varepsilon 1 + np^m) = n \wedge x_3(x^n \varepsilon 1 + np)$
 - 6 $a \in n \wedge x_3(x^n \varepsilon 1 + np) . \supset . a \uparrow p^{m-1} \varepsilon n \wedge x_3(x^n \varepsilon 1 + np^m)$
- {AMICI, *Sulla risoluzione etc.* Rend. d. Circolo M. di Palermo, t. 11, a. 1897, p. 44}

Plure propositiones de nn. 25, 26, 27 et sequentes pertine ad EULERO, v. Comm. Nov. Petrop. t. 7, p. 49; t. 18. p. 85 et Opusc. Analytica, t. 1.

* 28. $n, m \in \mathbb{N}_1 . \supset$:

- 1 $n \wedge x_3(x^n \varepsilon 1 + 2^m n) = n \wedge x_3(x \uparrow D(n, 2^m) \varepsilon 1 + 2^m n)$
- 2 $m \in \mathbb{N}_1 + 2 . n \in 1 \cdots (m - 2) . \supset .$
 $\text{Num}[1 \cdots (2^n - 1) \wedge x_3(x \uparrow 2^n \varepsilon 1 + n 2^m)] = 2^{n+1}$
- 3 $\text{Hp} 2 . \supset . 1 \cdots (2^n - 1) \wedge x_3(x \uparrow 2^n \varepsilon 1 + n 2^m) =$
 $1 + 2^{m-2} \times [0 \cdots (2^n - 1)] \vee -1 + 2^{m-n} \times (1 \cdots 2^n)$

* 29. $p \in \mathbb{N}_{p-1} . n \in \mathbb{N}_1 . a \in n - np . \supset$:

- 1 $\mathbb{Q} n \wedge x_3(x^n \varepsilon a + np) . = . a \uparrow [(p-1) / D(n, p-1)] \varepsilon 1 + np$
 - 2 $\text{Hp} 1 . \supset . \text{Num}[1 \cdots (p-1) \wedge x_3(x^n \varepsilon a + np)] = D(n, p-1)$
- {GAUSS, Disqu. Arith., art. 60 et sequ.; LEGENDRE, *Essai etc.*, 2^e éd., n. 334}
- 3 $r \in \mathbb{N}_1 \wedge x_3[nx \uparrow D(n, p-1) \varepsilon 1 + n(p-1) / D(n, p-1)] . \supset .$
 $n \wedge x_3(x^n \varepsilon a + np) = n \wedge x_3(x \uparrow D(n, p-1) \varepsilon a^r + np)$

GAUSS indica cum $\gamma a \pmod{p}$ numeros que satisfac ad congruentia $x^n \equiv a + np$. Ce espressione habe aut nullo aut uno aut plure valore incongruo \pmod{p} . Hodie nullo auctore ute ce notatione.

$$\cdot 4 \quad u \in n . \min[N_1 \wedge x_3(u^n \equiv 1 + np)] = n . k \in n \wedge x_3(x^n \equiv a + np) . \supset . \\ n \wedge x_3(x^n \equiv a + np) = (ku^n + np) | r^{1 \cdots n}$$

{GAUSS, Disqu. Arith., art. 65, 1^o.}

$$\cdot 5 \quad n \in N_1 \wedge (p-1)/N_1 . D[n, (p-1)/n] = 1 . a \nmid [(p-1)/n] \equiv 1 + np . \\ r \in N_1 \wedge x_3[nx \equiv 1 + n(p-1)/n] . \supset . a^r \equiv n \wedge x_3(x^n \equiv a + np)$$

{GAUSS, Disqu. Arith., art. 67.}

Circa conatus ut inveni solutiones de congruentia $x^n \equiv a + np$, ubi $n \in N_1 \wedge (p-1)/N_1$, v. GAUSS, D. A. art. 67, 68, LEGENDRE, E. 2^e éd. p. 354 (n. 342), p. 355, (n. 346).

$$\cdot 6 \quad \nexists n \wedge x_3(x^n + 1 \equiv np) . = . (p-1)/D(n, p-1) \equiv 2N_0 + 1$$

$$\cdot 7 \quad n \wedge x_3(x^n + 1 \equiv np) = n \wedge x_3[x \nmid D(n, p-1) + 1 \equiv np]$$

* 30. $p \in N_{p-2} . m \in N_1 . a \equiv n - np . \supset .$

$$\cdot 1 \quad \nexists n \wedge x_3(x^n \equiv a + np^m) . = . a \nmid [\Phi p^m / D(n, \Phi p^m)] \equiv 1 + np^m$$

$$\cdot 2 \quad r \in N_1 \wedge x_3[nx / D(n, \Phi p^m) \equiv 1 + \Phi p^m / D(n, \Phi p^m)] . \supset . \\ n \wedge x_3(x^n \equiv a + np^m) = n \wedge x_3[x \nmid D(n, \Phi p^m) \equiv a^r + np^m]$$

$$\cdot 3 \quad n \in N_1 \wedge \Phi p^m / N_1 . \supset . \nexists n \wedge x_3(x^n \equiv a + np^m) . = . \\ a \nmid \{[(p-1)p \nmid \text{mp}(p, n)]/n\} \equiv 1 + np \nmid [\text{mp}(p, n) + 1]$$

$$\cdot 4 \quad n \in N_1 \wedge \Phi p^m / N_1 . \nexists n \wedge x_3(x^n \equiv a + np^m) . \supset .$$

$$n \wedge x_3(x^n \equiv a + np^m) = \{x + yp \nmid [m - \text{mp}(p, n)] + np^m\} | x, 1 \cdots (p^m - 1) \\ \wedge x_3[x^n \equiv a + np^m . \nexists z_3(z^n \equiv a + np . x \equiv z + np)] , y, 0 \cdots [p \nmid \text{mp}(p, n) - 1]$$

$$\cdot 5 \quad \text{Hp}^4 . \supset . \text{Num}[1 \cdots (p^m - 1) \wedge x_3(x^n \equiv a + np^m)] = D(n, \Phi p^m)$$

$$\cdot 6 \quad \text{Hp}^4 . k \in n \wedge x_3(x^n \equiv a + np^{m-1}) . r = \text{mp}(p, n) . \supset : \\ r < m-1 . h \in n \wedge x_3[(k^n - a)/p^{m-1} + xk^{n-1}n/p^r \equiv np] . \supset . \\ k + hp^{n-r-1} \equiv n \wedge x_3(x^m \equiv a + np^m)$$

$$\cdot 7 \quad \text{Hp}^4 . k \in n \wedge x_3(x^n \equiv a + np^{m-1}) . \text{mp}(p, n) = m-1 . \supset . \\ n \wedge x_3(x^n \equiv a + np^m) = n \wedge x_3(x^n \equiv a + np)$$

$$\cdot 8 \quad n \in N_1 \wedge (p-1)/N_1 . k \in n \wedge x_3(x^n \equiv a + np) . \supset . \\ \{a \nmid [p^m - 2p^{m-1} + 1]/n\} | k \nmid p^{m-1} \equiv n \wedge x_3(x^n \equiv a + np^m)$$

{v. meo scripto, *Applicazione* etc., Napoli R., 1904, n. 7, nota}

* 31. $m, n \in N_1 . a \in 2n+1 \ . \supset :$

⁷⁸ 1. $\exists n \wedge x \exists (x^n \in a + n2^m) . = . a \nmid [\Psi 2^m / D(n, \Psi 2^m)] \in 1 + n2^m$

2. $r \in N_0 \wedge x \exists [n x \in D(n, \Psi 2^m) + n \Psi 2^m] \ . \supset .$

$n \wedge x \exists (x^n \in a + 2^m n) = n \wedge x \exists [x \nmid D(n, \Psi 2^m) \in a' + 2^m n]$

3. $n \in 2N_0 + 1 . m \in N_1 + 1 . k \in N_0 \wedge x \exists (2^{m-2} x \in -1 + mn) \ . \supset .$

$a \nmid [(2^{m-2} k + 1) / n] \in n \wedge x \exists (x^n \in a + 2^m n)$

{AMICI, *Sulla risoluzione*, etc., Rend. d. Circolo M. di Palermo, t. 11, a. 1897, p. 46}

4. $n \in N_1 . m \in N_0 + n + 2 \ . \supset . \exists n \wedge x \exists (x \nmid 2^n \in a + 2^m n) . = . a \in 1 + 2^{n+2} n$

{AMICI, *Risoluzione*, etc., Rend. d. Circolo M. di Palermo, t. 8, a. 1894, p. 198}

5. $Hp.4 . a \in 1 + 2^{n+2} n . s = mp(2, a-1) \ . \supset .$

$(a + 2^n - 1) / 2^n - \sum \{ [(1-a)/2^n]^r / r! I[2^n x - 1 | x, 1^{r-1}] \} | r, 2^{n-1} E[(m-2)/(s-n-1)] \in n \wedge x \exists (x \nmid 2^n \in a + 2^m n)$

{Vide meo scripto: *Estensione* etc., Napoli R., 1905}

6. $Hp.4 . a \in 1 + 2^{n+2} n \ . \supset .$

$Num[1^{n-1} (2^m - 1) \wedge x \exists (x \nmid 2^n \in a + 2^m n)] = 2^{n+1}$

{AMICI, *Risoluzione*, etc., Rend. d. Circolo di Palermo, t. 8 a. 1894, p. 198}

7. $Hp.6 . v \in n \wedge x \exists (x \nmid 2^n \in a + 2^m n) \ . \supset .$

$n \wedge x \exists (x \nmid 2^n \in a + 2^m n) = (v + 2^{m-n} n) \vee -v + 2^{m-n} n$

§7. Theoria de gaussiano. Radices primitivo. Indices

* 32. $a \in n . m \in N_1 . D(a, m) = 1 \ . \supset .$

0. $gss(m, n) = \min[N_1 \wedge x \exists (a^v \in 1 + nm)]$

Df gss

$gss(m, n)$ = gaussiano de m in basi n . Vocabulo « gaussiano » es introducto a LUCAS, sed ce auctore appella tali numero « gaussiano de n secundum modulo m » (Théor. d. Nombres, 1901, p. 439) GAUSS appella illo « exponente ad que n

pertine ». Circa omni theoria de gaussiano v. meo articulo, *Sui numeri composti*, etc., Ann. di Mat. (s. 3^o, t. 9, a. 1903, p. 139).

$$\cdot 1 \quad N_0 \wedge x \exists (a^x \varepsilon 1 + nm) = N_0 \times \text{gss}(m, a)$$

$$\cdot 2 \quad r, s \in N_0 \quad \supset: a^r \varepsilon a^s + nm \quad . = . \quad r \varepsilon s + n \times \text{gss}(m, a)$$

$$\ast \quad 33. \quad a \varepsilon 4n + 3 - 1 \quad . \quad m \in N_1 \quad . \quad n = \text{mp}(2, a + 1) \quad \supset:$$

$$\cdot 1 \quad \text{gss}(2, a) = 1$$

$$\cdot 2 \quad m \varepsilon 2^{n+1} \quad \supset. \quad \text{gss}(2^m, a) = 2$$

$$\cdot 3 \quad m > n \quad \supset. \quad \text{gss}(2^m, a) = 2^{m-n}$$

$$\ast \quad 34. \quad a \varepsilon 4n + 1 - 1 \quad . \quad m \in N_1 \quad . \quad n = \text{mp}(2, a - 1)$$

$$\cdot 1 \quad m \leq n \quad \supset. \quad \text{gss}(2^m, a) = 1$$

$$\cdot 2 \quad m \geq n \quad \supset. \quad \text{gss}(2^m, a) = 2^{m-n}$$

$$\ast \quad 35. \quad p \varepsilon N_{p-2} \quad . \quad a, b \varepsilon n - np \quad \supset:$$

$$\cdot 1 \quad \text{gss}(p, a) \varepsilon N_1 \wedge (p-1)/N_1$$

{FERMAT, a.1640, Oeuvres, t. 2, p. 209}

$$\cdot 2 \quad \text{Num}[1 \cdots (p-1) \wedge x \exists (a^x \varepsilon b + np)] = (p-1)/\text{gss}(p, a)$$

$$\cdot 3 \quad k, l \in N_0 \wedge x \exists (a^x \varepsilon b + np) \quad \supset: \quad k \varepsilon l + n \times \text{gss}(p, a)$$

Ce P es in Form 1902 (§Np.10.1) sub forma pauco diverso.

$$\ast \quad 36. \quad p \varepsilon N_{p-2} \quad . \quad a \varepsilon n - np \quad . \quad n = \text{mp}[p, a \wedge \text{gss}(p, a) - 1] \quad . \quad m \in N_1 \quad \supset:$$

$$\cdot 1 \quad m \leq n \quad \supset. \quad \text{gss}(p^m, a) = \text{gss}(p, a)$$

$$\cdot 2 \quad m \geq n \quad \supset. \quad \text{gss}(p^m, a) = p^{m-n} \text{gss}(p, a)$$

$$\cdot 3 \quad \text{gss}(p^m, a) \varepsilon N_1 \wedge p^{m-1}(p-1)/N_1$$

$$\ast \quad 37. \quad a \varepsilon n \quad . \quad m, n \in N_1 \quad . \quad D(m, n) = D(a, m) = D(a, n) = 1 \quad \supset.$$

$$\cdot 1 \quad \text{gss}(mn, a) = \text{mlt}[\text{gss}(m, a), \text{gss}(n, a)]$$

$$\cdot 2 \quad \text{gss}(m, a) = \text{mlt}[\text{gss}(x, a) | x, (Np \uparrow N_1) \wedge m/N_1]$$

$$\cdot 3 \quad \text{gss}(m, a) \varepsilon N_1 \wedge \Psi m/N_1$$

* 38. $p \in Np-12$

$$\cdot 0 \quad Rprp = n^{\wedge} x3 [gss(p, x) = p-1] \quad \text{Df Rpr}$$

$Rprp = \text{radice primitivo de } p$, es numero que pertenece ad exponente $p-1$, secundum modulo p . Ce denominatione es introducto ab EULERO.

$$\cdot 1 \quad \text{Num}[1 \cdots (p-1) \wedge Rprp] = \Phi(p-1)$$

EULERO primo demonstra existe radice primitivo de p , sed suo demonstratione habe aliquo mendo (Comm. n. Ae. Petrop. t. 18, p. 85. Primo demonstratione completo pertine ad GAUSS (Disqu. Arith., art. 55).

$$\cdot 2 \quad Rprp = n^{\wedge} x3 \{ a3 Np \wedge (p-1)/N_1 \cdot \bigcup_a. x \nmid [(p-1)/a] - 1 \varepsilon np \}$$

$$\cdot 3 \quad Rprp = n^{\wedge} x3 [a \varepsilon Np \wedge (p-1)/N_1 \cdot \bigcup_a. \neg \exists y3(y^a \varepsilon x + np)]$$

$$\cdot 4 \quad \begin{aligned} & a \varepsilon n - np \cdot gss(p, a) < p-1 \cdot b \varepsilon n - np \wedge x3 [r \varepsilon N_1 \cdot \bigcup_r. \\ & a^r \varepsilon x + np \cdot \bigcup: m \varepsilon N_1 \wedge gss(p, a)/N_1 \cdot n \varepsilon N_1 \wedge gss(p, b)/N_1 \cdot \\ & D(m, n) = 1 \cdot \text{mlt}[gss(p, a), gss(p, b)] = mn \cdot \bigcup. \\ & \{ a \nmid [gss(p, a)/m] \} \{ b \nmid [gss(p, b)/n] \varepsilon n^{\wedge} x3 [gss(p, x) > gss(p, a)] \end{aligned}$$

In generali oportet conatu ut inveni uno radice primitivo de p , et EULERO puta es difficili inveni tali numero (Opusc. Analyt., t. 1, p. 152). In aliquo easu applicatione de P.2.3 es utile.

Ex P.4 GAUSS trahe methodo ut inveni uno radice primitivo de p (Disqu. Arith., n. 73). Circa alio methodo v. OLTRAMARE, J. f. Math. t. 49, a.1855, p. 161; FROLOV, Bull. Soe. math. de France t. 21, a.1893, p. 113; t. 22, a.1894, p. 211.

$$\cdot 5 \quad p \in Np-13 \cdot \bigcup. \Pi[1 \cdots (p-1) \wedge Rprp] \varepsilon 1 + N_0 p$$

$$\cdot 6 \quad p-1 \varepsilon N_1 \times (N_1 + 1)^2 \cdot \bigcup. \Sigma[1 \cdots (p-1) \wedge Rprp] \varepsilon np$$

$$\cdot 7 \quad p-1 \varepsilon N_1 \times (N_1 + 1)^2 \cdot \bigcup. \Sigma[1 \cdots (p-1) \wedge Rprp] \varepsilon (-1) \wedge \text{Num}[Np \wedge (p-1)/N_1] + np$$

{ 3.6.7 GAUSS, Disqu. Arith. art. 80, 81 v. et ARNDT, J. f. Math. t. 31, a.1846, p. 326; HOFMANN, Math. Ann. t. 20, a.1882, p. 471 }

$$\begin{aligned} * \quad 39 \cdot 0 \quad & a \varepsilon n - np \cdot u \varepsilon \text{Cls}'Np \cdot \bigcup: \\ & a \varepsilon Rpru \cdot ==: x \varepsilon u \cdot \bigcup_c. a \varepsilon Rprx \end{aligned}$$

Df

- 1 $3, 5, 6, 10 \in \text{Rpr}\{Np \wedge [2 \nmid (2 \nmid N_i) + 1]\}$
 - 2 $2 \in \text{Rpr}[Np \wedge 2(Np \wedge 4N_0 + 1) + 1]$
 - 3 $-2 \in \text{Rpr}[Np \wedge 2(Np \wedge 4N_0 + 3) + 1]$
 - 4 $2 \in \text{Rpr}[Np \wedge 4Np + 1]$
- 1...4, v. TCHEBYCHEF, *Teoria delle congruenze* (trad. MASSARINI) pp. 209-213]

·5 $m \in N_i + 1 \supset 3 \in \text{Rpr}\{Np \wedge 2^m[Np \wedge N_i + (9 \nmid 2^{m-2} - 1)/2^{m+1}] + 1\}$
 {Ce} P es in theoria de congruentias de TCHEBYCHEF (trad. MASSARINI, p. 212) sub forma minus utile. In ce forma es in
 « *Elém. de la th. des nombres*, par E. CAHEN, p. 398 }

Existe tabulas de radice primitivo, v.

TCHEBYCHEF, *Teoria delle congruenze* (trad. MASSARINI).
Turola delle radici primitive dei numeri primi da 3 a 353,
 (pp. 248-287).

WERTHEIM, *Primitive Wurzeln des Primzahlen* $2^q + 1$, bei
 Welchen $q=1$, oder gleich einer ungeraden Primzahl ist;
 Zeitsch. f. Math., t. 25, a.1894, pp. 81-97; — *Tabelle der klein-
 sten primitiven Wurzeln g aller ungeraden Primzahlen p unter
 3000*, Acta Math., t. 17, a.1893, pp. 315-320; — *Primitive Wur-
 zeln der Primzahlen von der Form* $2\pi q^2 + 1$ *in welcher* $q=1$
*oder eine ungerade Primzahl ist. Tabelle der kleinsten pri-
 mitiven Wurzeln g aller Primzahlen p zwischen 3000 und 10000*,
 Acta Math., t. 20, a.1896, pp. 143-157; — *Berichtigungen zur
 Tabelle der kleinsten primitiven Wurzeln unter 10000* (Acta
 Math., t. 22, 1898).

* 40. $p \in Np \wedge 2 \cdot a \in \text{Rpr} p \cdot b, c \in n \cdot np \supset$:

·0 ${}^a\text{Ind}(b, p) = \min[N_0 \wedge x \exists (a^x \in b + np)]$

${}^a\text{Ind}(b, p)$ = indice de b in basi a , secundum modulo p . Ce
 denominatione et symbolo « Ind » es introducto a GAUSS (Disqu.
 Arit. art. 57). Theoria de Indice es analogo ad theoria de
 logarithmo.

·1 ${}^a\text{Ind}(b, p) \in 0 \cdots (p-2)$

·2 $k \in n \wedge x \exists (a^x \in b + np) \supset k \in {}^a\text{Ind}(b, p) + n(p-1)$

·3 ${}^a\text{Ind}(1, p) = 0$

- 4 ${}^a\text{Ind}(a,p)=1$
- 5 $b \in c + np \supset {}^a\text{Ind}(b,p) \varepsilon {}^a\text{Ind}(c,p) + n(p-1)$
- 6 ${}^a\text{Ind}(bc,p) \varepsilon {}^a\text{Ind}(b,p) + {}^a\text{Ind}(c,p) + n(p-1)$
- 7 $m \in N_1 \supset {}^a\text{Ind}(b^m,p) \varepsilon m \times {}^a\text{Ind}(b,p) + n(p-1)$
- 8 $c \in \text{Rprp} \supset {}^c\text{Ind}(b,p) \times {}^a\text{Ind}(c,p) \varepsilon {}^a\text{Ind}(b,p) + n(p-1)$
- 9 $a \in \text{Rprp} \supset c \in N_1 \cdot D(c,p-1)=1 \supset a^c \in \text{Rprp}$

* 41. $p \in N_{p-2} \cdot a \in \text{Rprp} \cdot b, c \in n - np \supset$:

- 1 $\text{gss}(p,b) = (p-1)/D[(p-1), {}^a\text{Ind}(b,p)]$
- 2 $n \in N_1 \cdot k \in \wedge x \exists (bx^n \varepsilon c + np \supset$
 $n \times {}^a\text{Ind}(k,p) \varepsilon {}^a\text{Ind}(c,p) - {}^a\text{Ind}(b,p) + n(p-1)$

In propositione ·2 es uno methodo ut resolve congruentia binomio $bx^n \varepsilon c + np$ (v. ARNDT, J. f. math., t. 31, a.1846, p. 333). Ut applica ce methodo oportet tabulas de indice, pro que v. GAUSS, Disqu. Arith., tabula de indice de numero primo ex 3 usque ad 97; — T'CHEBYCHEF, Teoria delle congruenze (trad. MASSARINI), v. P 39·4.

* 42. $p \in N_{p-2} \cdot m \in N_1 \supset$

- 0 $\text{Rprp}^m = n \wedge x \exists [\text{gss}(p^m, x) = \Phi p^m]$ Df
- 1 $m \in N_1 + 1 \supset \text{Rprp}^m = \text{Rprp}^2$
- 2 $\text{Num}[1 \cdots (p^m - 1) \wedge \text{Rprp}^m] = \Phi \Phi p^m$

{LEBESGUE, J. de Math., t. 19, a.1854, p. 289, 334}

* 43. $m \in N_1 \cdot p \in N_{p-2} \cdot a \in \text{Rprp}^m \cdot b, c \in n - np \supset$:

- 0 ${}^a\text{Ind}(b,p) = \min[N_0 \wedge x \exists (a^x \varepsilon b + np^m)]$ Df
- 1 ${}^a\text{Ind}(b,p) \varepsilon 0 \cdots (\Phi p^m - 1)$
- 2 $k \in n \wedge x \exists (a^x \varepsilon b + np^m) \supset k \varepsilon {}^a\text{Ind}(b,p^m) + n \times \Phi p^m$
- 3 ${}^a\text{Ind}(1,p^m) = 0$
- 4 ${}^a\text{Ind}(a,p^m) = 1$
- 5 $b \varepsilon c + np^m \supset {}^a\text{Ind}(b,p^m) \varepsilon {}^a\text{Ind}(c,p^m) + n \times \Phi p^m$
- 6 ${}^a\text{Ind}(bc,p^m) \varepsilon {}^a\text{Ind}(b,p^m) + {}^a\text{Ind}(c,p^m) + n \times \Phi p^m$

- 7 $n \in N_1 \supset \text{"Ind}(b^m, p^m) \in n \times \text{"Ind}(b, p) + n \times \Phi p^m$
- 8 $c \in \text{Rpr} p^m \supset \text{"Ind}(b, p^m) \times \text{"Ind}(c, p^m) \in \text{"Ind}(b, p^m) + n \times \Phi p^m$
- 9 $c \in N_1 \cdot D(c, \Phi p^m) = 1 \supset a^c \in \text{Rpr} p^m$

* 44. Hp43 \supset :

- 1 $\text{gss}(p^m, b) = \Phi p^m / D[\Phi p^m, \text{"Ind}(b, p^m)]$
- 2 $n = \text{mp}[p, b \uparrow \text{gss}(p, b) - 1] \cdot m \leq n \supset \text{"Ind}(b, p^m) \in N_0 \times p^{n-1}$
- 3 $\text{-----} \cdot m \leq n \supset \text{-----} \in N_0 \times p^{m-1}$
- 4 $n \in N_1 \cdot k \in n \wedge x \exists (bx^n \in c + n p^m) \supset$
 $n \times \text{"Ind}(k, p^m) \in \text{"Ind}(c, p^m) - \text{"Ind}(b, p^m) + n \times \Phi p^m$

* 45. $m \in N_0 \supset$:

- 0 $\text{Rpr} 2^m = n \wedge x \exists [\text{gss}(2^m, x) = \Phi 2^m]$ Df
- 1 $\text{Rpr} 1 = n$
- 2 $\text{Rpr} 2 = 2n + 1$
- 3 $\text{Rpr} 4 = 4n - 1$
- 4 $m \in N_1 + 2 \supset \neg \exists \text{Rpr} 2^m$
- 5 $m \in N_1 \cdot b \in 2n + 1 \supset \exists (x, y) \exists [x, y \in N_0 \cdot b \in (-1)^x 5^y + n 2^m]$

{GAUSS, Disqu. Arith., art. 91}

* 46. $m \in \iota 0 \iota 1 \iota 2 \cdot a \in \text{Rpr} 2^m \cdot b \in 2n + 1 \supset$

- 0 $\text{"Ind}(b, 2^m) = \min[N_0 \wedge x \exists (a^x \in b + n 2^m)]$ Df
- 1 $\text{"Ind}(b, 1) = 0$
- 2 $a \in 2n + 1 \supset \text{"Ind}(b, 2) = 1$
- 3 $a \in 4n - 1 \supset \text{"Ind}(b, 4) \in \iota 0 \iota 1$

* 47·0 $m \in N_1 \cdot b \in 2n + 1 \supset \text{Ind}(b, 2^m) =$

$$n(x, y) \exists \{x \in \iota 0 \iota 1 \cdot y = \min N_0 \wedge y \exists [b \in (-1)^x 5^y + 2^m n]\} \quad \text{Df}$$

$\text{Ind}(b, 2^m)$ es appellato systema de indices de b secundum modulo 2^m . Si es $m \leq 2$, nos pote semper loque de systema de indices.

N. AMICI in articolo *Risoluzione della congruenza $x^m \equiv b \pmod{2^r}$* , Rend. Circolo Mat. di Palermo, t. 8, a. 1894, pp. 187-201,

appella « radice quasi primitivo di 2^n » numero que pertine ad exponente 2^{n-2} , et supra tali numeros pone fundamento de theoria de indices secundum modulo 2^n . Ipse ute ce methodo ut resolve congruentia $x^m \varepsilon b + 2^n n$, et $a^x \varepsilon b + 2^n n$, sed me inveni formula de resolutione pro congruentia $x^m \varepsilon b + 2^n n$, v. P31.3.

* 48. $m \in N_1 \supset$.

$$^0 \text{ Rprm} = n \wedge x3[\text{gss}(m, x) = \Phi m]$$

$$^1 \text{ Rprm} = m \varepsilon 1 \vee 2 \vee 4 \vee (Np-2) \wedge N_1 \vee 2(Np-2) \wedge N_1$$

{GAUSS, Disqu. Arith., art. 92}

Si m non habe radice primitivo, DIRICHLET defini systema de indices de m , Berl. Abh. a.1837, p. 45 = Werke, t. 1, p. 313, aut *Vorlesungen*, suppl. 5. — V. et BENNETT, London Trans., t. 184, a.1893, p. 189, ubi es et tabulas.

§ 8 Applicationes

* 49. $a \in N_1 \supset$:

$$^1 n \wedge x3(x^{n-1} \varepsilon 1 + na) =$$

$$n \wedge x3\{x \uparrow \text{mlt}[D(a, p-1) | p, Np \wedge a/N_1] - 1 \varepsilon na\}$$

$$^2 \text{ Num}[1 \cdots (a-1) \wedge x3(x^{n-1} \varepsilon 1 + na)] = H[D(a, p-1) | p, Np \wedge a/N_1]$$

$$^3 p, q \varepsilon Np-2 . a \varepsilon n^2 + nq - nq \supset . a \uparrow (pq-1) \varepsilon 1 + pqn$$

$$^{31} p \varepsilon Np \wedge 4N_1 + 3 . 2p-1 \varepsilon Np \supset . 3 \uparrow p(2p-1) \varepsilon 1 + N_1 \times p(2p-1)$$

$$^{32} p \varepsilon Np \wedge 4N_1 + 1 . 2p-1 \varepsilon Np \supset . 2 \uparrow p(2p-1) \varepsilon 1 + N_1 \times p(2p-1)$$

$$^{33} \text{ ————— } . \text{ ————— } \supset . 3 \uparrow p(2p-1) \varepsilon 1 + N_1 \times p(2p-1)$$

$$^{34} p \varepsilon Np \wedge 20N_0 + 1 . 2p-1 \varepsilon Np \supset . 10 \uparrow p(2p-1) \varepsilon 1 + N_1 \times p(2p-1)$$

{¹...³⁴ v. meo scripto, sui numeri composti etc., Annali di M., s. 3., t. 9, a.1903, pp. 139-160}

$$* \text{ } ^{50.1} p \varepsilon N_1 . a \varepsilon n . D(a, p) = 1 . \text{gss}(p, a) = p-1 \supset . p \varepsilon Np$$

{LUCAS, *Sur la recherche des grands nombres premiers*, Congrès de Clermont-Ferrand, a.1876}

$$^2 q \varepsilon Np \wedge 4N_0 + 1 \supset : 2q+1 \varepsilon Np = . 2^q + 1 \varepsilon N_1 \times (2q+1)$$

·3 $q \in Np \wedge 4N_0 + 3 \vdash: 2q + 1 \in Np \Rightarrow 2^q - 1 \in N_1 \times (2q + 1)$
 {LUCAS, Congrès du Havre, 1877}

·4 $q \in Np \vdash: 4q + 1 \in Np \Rightarrow$
 $2 \nmid q + 2 \nmid [(q + 1)/2] + 1 \vee 2 \nmid q - 2 \nmid [(q + 1)/2] + 1 \in N_0(4q + 1)$

·5 $m \in 2 \nmid N_1 \vdash: 2^m + 1 \in Np \Rightarrow 3 \nmid (2^m - 1) + 1 \in N_1 \times (2^m + 1)$
 {PROTH, Corr. N. a. 1878, t. 4, p. 210. Theoremas analogo circa
 numeros primo de forma $2^m + 1$ tradé PÉPIN, Compt. R.
 de l'A. de Paris, 1877, 2^o sem., p. 329. LUCAS tribue ad
 se ce P in praefatione de suo *Théorie des Nombres*,
 sed ibi. es errore typographico.

·6 $q \in Np \wedge 4N_0 + 3 \vdash: 6q + 1 \in Np \Rightarrow 2 \nmid 3q + 1 \in N_1 \times (6q + 1)$

·7 $q \in Np \wedge 4N_1 + 1 \vdash: 6q + 1 \in Np \Rightarrow 2 \nmid 3q - 1 \in N_1 \times (6q + 1)$

·8 $m \in N_1 + 1 \cdot q \in Np \wedge [N_1 + (9 \nmid 2^{m-1} - 1)/2^{m+1}] \vdash:$
 $2^m q + 1 \in Np \Rightarrow 3 \nmid 2^{m-1} q + 1 \in N_1 \times (2^m q + 1)$

Vide meo scripto *Delle congruenze binomie* etc., Periodico
 di Mat., 1903, p. 330.

P·3 es in F1902, §Np7·4, sed non in forma completo.

P·5 = F1902, §Np7·2.



